Random dimension reduction

& learning symmetric properties of quantum states

Angus Lowe & Xinyu (Norah) Tan

MIT

arxiv:2606.23592

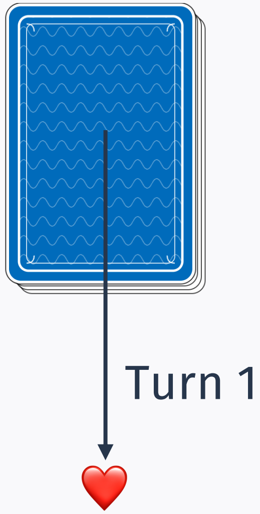
Results

We study a quantum channel that simultaneously reduces the dimensions of multiple input states while preserving certain symmetric properties of the input.

This leads to improved upper bounds for several quantum learning tasks.

This also completes the story for optimal quantum tomography without representation theory.

Learning symmetric properties

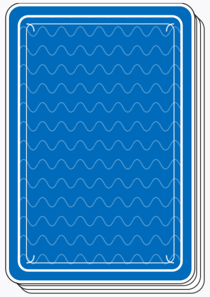


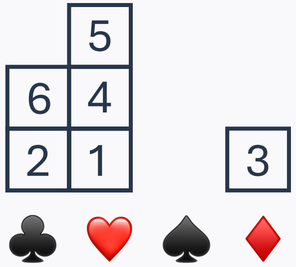
$\boxed{1}$

♣ ♥ ♠ ♦

Learning symmetric properties

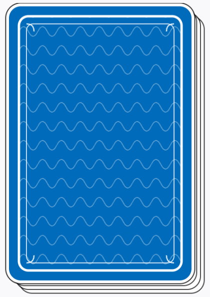
Learning symmetric properties

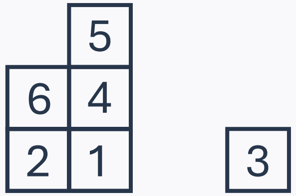




- We say a property is *symmetric* if its value does not depend on the labels
    - E.g., invariance under ♣↔❤️

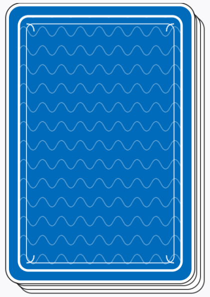
Learning symmetric properties

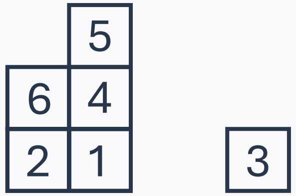




- We say a property is *symmetric* if its value does not depend on the labels
  - E.g., invariance under ♣↔❤️

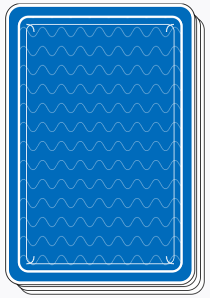
Learning symmetric properties

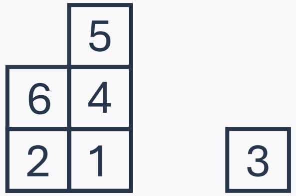




- We say a property is *symmetric* if its value does not depend on the labels
  - E.g., invariance under ♣↔❤️
- This symmetry appears when estimating [VV'11,WY'16]:
  - Entropy
  - Support size

Learning symmetric properties

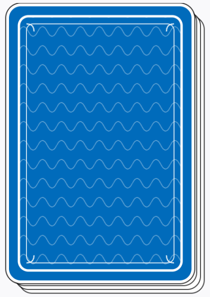


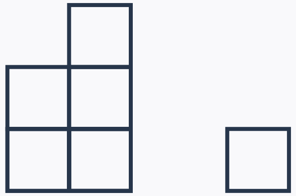


- We say a property is *symmetric* if its value does not depend on the labels
  - E.g., invariance under ♣ ↔ ❤️
- This symmetry appears when estimating [VV’11,WY’16]:
  - Entropy
  - Support size

contents 1,2,... etc also irrelevant

Learning symmetric properties

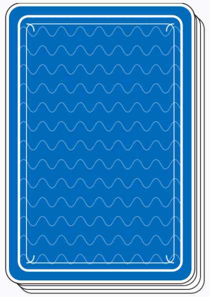


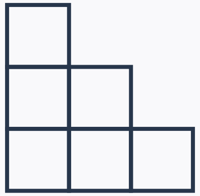


- We say a property is *symmetric* if its value does not depend on the labels
  - E.g., invariance under ♣↔❤️
- This symmetry appears when estimating [VV'11,WY'16]:
  - Entropy
  - Support size

contents 1,2,... etc also irrelevant

Learning symmetric properties

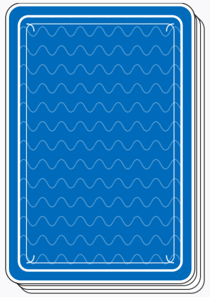


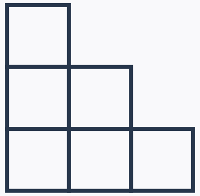


- We say a property is *symmetric* if its value does not depend on the labels
    - E.g., invariance under ♣ ↔ ❤️
- This symmetry appears when estimating [VV'11,WY'16]:
    - Entropy
    - Support size

contents 1,2,... etc also irrelevant

Learning symmetric properties

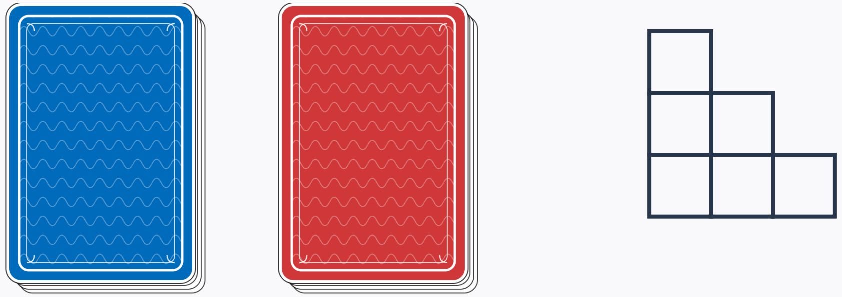




- We say a property is *symmetric* if its value does not depend on the labels
  - E.g., invariance under ♣↔❤️
- This symmetry appears when estimating [VV'11,WY'16]:
  - Entropy
  - Support size
  - Closeness of two distributions

contents 1,2,... etc also irrelevant

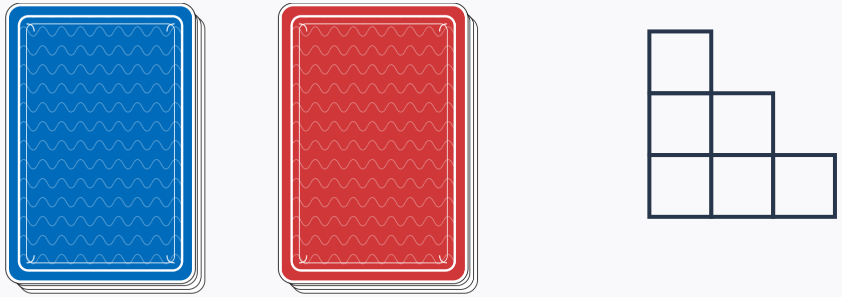
Learning symmetric properties



- We say a property is *symmetric* if its value does not depend on the labels
  - E.g., invariance under ♣↔❤️
- This symmetry appears when estimating [VV'11,WY'16]:
  - Entropy
  - Support size
  - Closeness of two distributions

contents 1,2,... etc also irrelevant

Learning symmetric properties

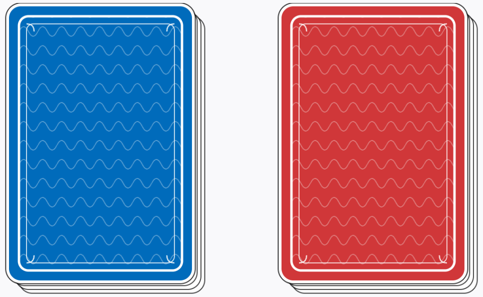


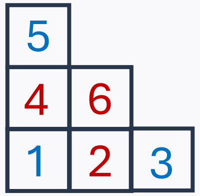
- We say a property is *symmetric* if its value does not depend on the labels
    - E.g., invariance under ♣ ↔ ❤️
- This symmetry appears when estimating [VV'11,WY'16]:
    - Entropy
    - Support size
    - Closeness of two distributions

contents 1,2,… etc also irrelevant

contents 1,2,… etc *are relevant again*

Learning symmetric properties





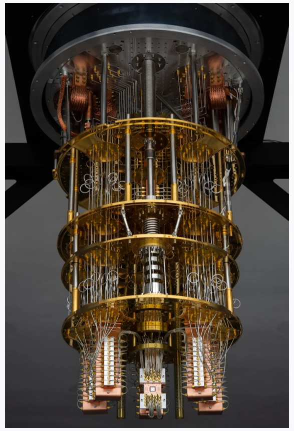
- We say a property is *symmetric* if its value does not depend on the labels
  - E.g., invariance under ♣↔❤️
- This symmetry appears when estimating [VV'11,WY'16]:
  - Entropy
  - Support size
  - Closeness of two distributions

contents 1,2,... etc also irrelevant

contents 1,2,... etc *are relevant again*

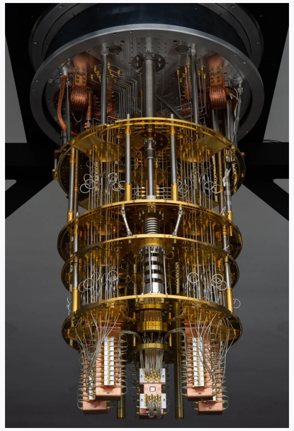
VV'11 – Valiant & Valiant. Estimating the unseen... (STOC'11)
WY'16 – Wu & Yang. Chebyshev polynomials... (Ann. Statist. 47(2))

Symmetric quantum properties



$$\longrightarrow \rho^{\otimes n}$$

Symmetric quantum properties



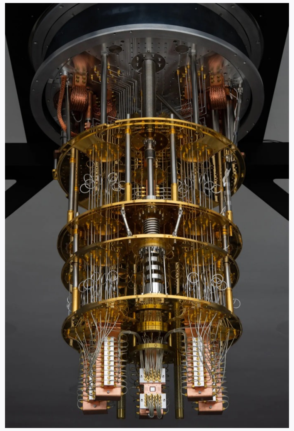
$\longrightarrow$ $\rho^{\otimes n}$

Problem (Entropy estimation)

Given: n copies of $\rho \in \mathbb{C}^{d\times d}$ with eigenvalues $\lambda_1 \geq \cdots \geq \lambda_r \geq \lambda_{r+1} = 0$

Output: Estimate of the von Neumann entropy $S(\rho) = -\operatorname{tr}(\rho \log \rho)$

Symmetric quantum properties



$\longrightarrow$ $\rho^{\otimes n}$

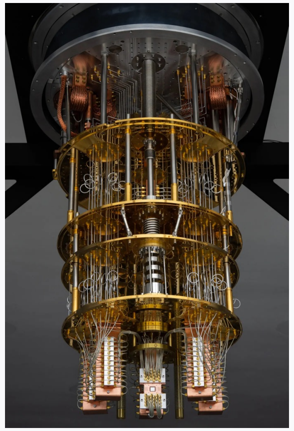
Problem (Entropy estimation)

Given: n copies of $\rho \in \mathbb{C}^{d\times d}$ with eigenvalues $\lambda_1 \geq \cdots \geq \lambda_r \geq \lambda_{r+1} = 0$

Output: Estimate of the von Neumann entropy $S(\rho) = -\operatorname{tr}(\rho \log \rho)$

Symmetric property: we have $S(W\rho W^\dagger) = S(\rho)$ for any isometry W

Symmetric quantum properties



$\longrightarrow \rho^{\otimes n}$

Problem (Entropy estimation)

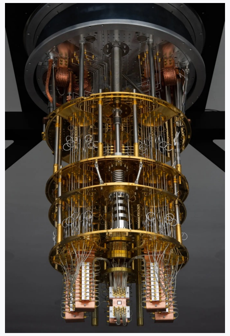
Given: n copies of $\rho \in \mathbb{C}^{d\times d}$ with eigenvalues $\lambda_1 \geq \cdots \geq \lambda_r \geq \lambda_{r+1} = 0$

Output: Estimate of the von Neumann entropy $S(\rho) = -\operatorname{tr}(\rho \log \rho)$

Symmetric property: we have $S\left(W\rho W^\dagger\right) = S(\rho)$ for any isometry W

Input state symmetry: $\rho^{\otimes n}$ invariance under S_n group action

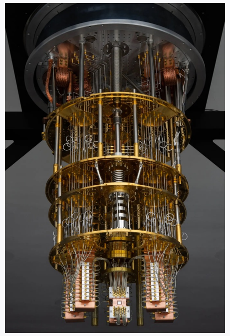
Symmetric quantum properties



$\longrightarrow \quad \rho^{\otimes n}$

$\longrightarrow \quad \sigma^{\otimes n}$

Symmetric quantum properties



$\longrightarrow \rho^{\otimes n}$

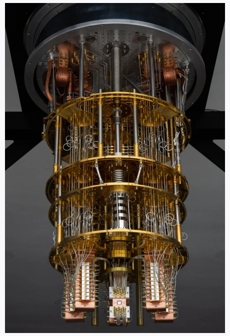
$\longrightarrow \sigma^{\otimes n}$

Problem (Fidelity estimation)

Given: n copies of $\rho \in \mathbb{C}^{d\times d}$ and n copies of $\sigma \in \mathbb{C}^{d\times d}$

Output: estimate of $F(\rho,\sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$

Symmetric quantum properties



$\longrightarrow$ $\rho^{\otimes n}$

$\longrightarrow$ $\sigma^{\otimes n}$

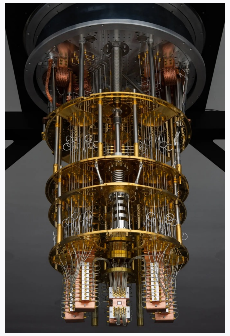
Problem (Fidelity estimation)

Given: n copies of $\rho \in \mathbb{C}^{d\times d}$ and n copies of $\sigma \in \mathbb{C}^{d\times d}$

Output: estimate of $F(\rho,\sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$

Symmetric property: we have $F\left(W\rho W^\dagger, W\sigma W^\dagger\right) = F(\rho,\sigma)$ for any isometry W

Symmetric quantum properties



$\rho^{\otimes n}$

$\sigma^{\otimes n}$

Problem (Fidelity estimation)

Given: n copies of $\rho \in \mathbb{C}^{d \times d}$ and n copies of $\sigma \in \mathbb{C}^{d \times d}$

Output: estimate of $F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$

Symmetric property: we have $F\left(W\rho W^\dagger, W\sigma W^\dagger\right) = F(\rho, \sigma)$ for any isometry W

Input state symmetry: $\rho^{\otimes n} \otimes \sigma^{\otimes n}$ is *not* invariant under S_{2n} group action

Symmetric quantum properties

Definition

A property f of a quantum state is *symmetric* if $f\left(W\rho W^\dagger\right) = f(\rho)$ for every isometry W.

E.g., *von Neumann entropy, rank*

Symmetric quantum properties

Definition

A property f of a quantum state is *symmetric* if $f\left(W\rho W^{\dagger}\right) = f(\rho)$ for every isometry W.

E.g., *von Neumann entropy, rank*

Definition

A property f of two quantum states is *symmetric* if $f\left(W\rho W^{\dagger}, W\sigma W^{\dagger}\right) = f(\rho, \sigma)$ for every isometry W.

E.g., *trace distance, fidelity*

Symmetric quantum properties

Definition

A property f of a quantum state is *symmetric* if $f\left(W\rho W^{\dagger}\right) = f(\rho)$ for every isometry W.

E.g., *von Neumann entropy, rank*

Definition

A property f of two quantum states is *symmetric* if $f\left(W\rho W^{\dagger}, W\sigma W^{\dagger}\right) = f(\rho, \sigma)$ for every isometry W.

E.g., *trace distance, fidelity*

Applications: *verification [Elb+'20], probing entanglement [SW'22,LL'26], quantum algorithms [CHW'07]*

[Elb+'20] - Elben et al. Cross-platform verification... (PRL 124(1))

[SW'22] – Soleimanifar & Wright. Testing matrix product states. (SODA'22)

[LL'26] – Lovitz & Lowe. Testing tree tensor network states (IEEE ToIT 72.5)

[CHW'07] – Weak Fourier Schur sampling... (STACS 2007)

Symmetric quantum properties

Definition

A property f of a quantum state is *symmetric* if $f\left(W\rho W^{\dagger}\right) = f(\rho)$ for every isometry W.

E.g., *von Neumann entropy, rank* $\leq$ $\boxed{\text{spectrum learning}}$

Definition

A property f of two quantum states is *symmetric* if $f\left(W\rho W^{\dagger}, W\sigma W^{\dagger}\right) = f(\rho, \sigma)$ for every isometry W.

E.g., *trace distance, fidelity*

Applications: *verification [Elb+'20], probing entanglement [SW'22,LL'26], quantum algorithms [CHW'07]*

[Elb+'20] - Elben et al. Cross-platform verification... (PRL 124(1))

[SW'22] – Soleimanifar & Wright. Testing matrix product states. (SODA'22)

[LL'26] – Lovitz & Lowe. Testing tree tensor network states (IEEE ToIT 72.5)

[CHW'07] – Weak Fourier Schur sampling... (STACS 2007)

Spectrum learning

Problem (Spectrum learning)

Given: n copies of a quantum state $\rho \in \mathbb{C}^{d\times d}$ with eigenvalues $\lambda_1 \geq \cdots \geq \lambda_r \geq \lambda_{r+1} = 0$

Output: $\hat{\lambda}$ which is close in TV distance to $(\lambda_1, \dots, \lambda_d)$.

Spectrum learning

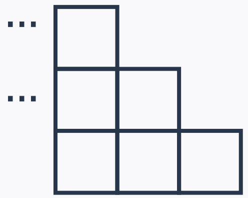
Problem (Spectrum learning)

Given: n copies of a quantum state $\rho \in \mathbb{C}^{d\times d}$ with eigenvalues $\lambda_1 \geq \cdots \geq \lambda_r \geq \lambda_{r+1} = 0$

Output: $\hat{\lambda}$ which is close in TV distance to $(\lambda_1, \dots, \lambda_d)$.

Step 1: Weak Schur sampling

$$\rho^{\otimes n} \cong \bigoplus_{\lambda \vdash n} I_{\mathcal{P}_\lambda} \otimes q_\lambda^d(\rho)$$



irreps of $\mathcal{S}_n$ and $\mathbb{U}(d)$

Spectrum learning

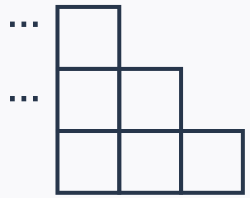
Problem (Spectrum learning)

Given: n copies of a quantum state $\rho \in \mathbb{C}^{d\times d}$ with eigenvalues $\lambda_1 \geq \cdots \geq \lambda_r \geq \lambda_{r+1} = 0$

Output: $\hat{\lambda}$ which is close in TV distance to $(\lambda_1, \ldots, \lambda_d)$.

Step 1: Weak Schur sampling

$$\rho^{\otimes n} \cong \bigoplus_{\lambda \vdash n} I_{\mathcal{P}_\lambda} \otimes q_\lambda^d(\rho)$$



irreps of $\mathcal{S}_n$ and $\mathbb{U}(d)$

Step 2: Empirical Young diagram [KW'01] $\longrightarrow$ $O(r^2)$ copies suffice[1] $\boxed{\textit{independent of } d}$

[1]Recently (last week) improved to $O\left(r^2 \frac{\log\log r}{\log r}\right)$ [PSTW'26]

[PSTW'26] – Pelecanos, Spilecki, Tang, Wright. The Keyl-Werner algorithm is not optimal... (2026)

Dimension independence via random purification

Q: is there another way to see that $O(r^2)$ is the right "baseline" for symmetric properties?

Dimension independence via random purification

Q: is there another way to see that $O(r^2)$ is the right "baseline" for symmetric properties?

Theorem (Random purification channel [TWZ'25])

$\forall r\ \exists$ a channel $\mathcal{P}^{(r)}$ with the action

$$\mathcal{P}^{(r)}\left(\rho^{\otimes n}\right) = \mathbb{E}_{\phi^\rho} |\phi^\rho\rangle\langle\phi^\rho|^{\otimes n}$$

for any quantum state ρ of rank at most r where $|\phi^\rho\rangle \in \mathbb{C}^d \otimes \mathbb{C}^r$ is a random purification, satisfying $\mathrm{tr}_2(|\phi^\rho\rangle\langle\phi^\rho|) = \rho$

If $\rho = \sum_{i=1}^{r} \lambda_i |\psi_i\rangle\langle\psi_i|$,

$|\phi^\rho\rangle = \sum_{i=1}^{r} \sqrt{\lambda_i}\, |\psi_i\rangle \otimes |\phi_i\rangle$

Dimension independence via random purification

Q: is there another way to see that $O(r^2)$ is the right "baseline" for symmetric properties?

Theorem (Random purification channel [TWZ'25])

$\forall r\ \exists$ a channel $\mathcal{P}^{(r)}$ with the action

$$\mathcal{P}^{(r)}\left(\rho^{\otimes n}\right) = \mathbb{E}_{\phi^\rho} |\phi^\rho\rangle\langle\phi^\rho|^{\otimes n}$$

for any quantum state ρ of rank at most r where $|\phi^\rho\rangle \in \mathbb{C}^d \otimes \mathbb{C}^r$ is a random purification, satisfying $\mathrm{tr}_2(|\phi^\rho\rangle\langle\phi^\rho|) = \rho$

If $\rho = \sum_{i=1}^r \lambda_i\, |\psi_i\rangle\langle\psi_i|$,

$|\phi^\rho\rangle = \sum_{i=1}^r \sqrt{\lambda_i}\, |\psi_i\rangle \otimes |\phi_i\rangle$

$$\rho^{\otimes n} \xrightarrow{\ \mathcal{P}^{(r)}\ } |\phi^\rho\rangle\langle\phi^\rho|^{\otimes n} \xrightarrow{\ \mathrm{tr}_1\ } \rho_0^{\otimes n} \qquad \rho_0 \in \mathbb{C}^{r\times r}, \quad \mathrm{spec}(\rho) = \mathrm{spec}(\rho_0)$$

Recall: Full state tomography has sample complexity $O(\dim(\rho_0)^2)$ [HHJWY'16, OW'16]

[HHJWY'16] – Haah et al. Sample-optimal quantum state tomography. (STOC'16)

[OW'16] – O'Donnell & Wright. Efficient quantum tomography. (STOC'16)

[TWZ'25] – Tang, Wright, Zhandry. Conjugate queries can help. (2025)

Limitations of random purification

Problem (Fidelity estimation)

Given: n copies of $\rho \in \mathbb{C}^{d\times d}$ and n copies of $\sigma \in \mathbb{C}^{d\times d}$

Output: estimate of $F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$

Limitations of random purification

Problem (Fidelity estimation)

Given: n copies of $\rho \in \mathbb{C}^{d\times d}$ and n copies of $\sigma \in \mathbb{C}^{d\times d}$

Output: estimate of $F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$

If ρ and σ both have rank at most r, then $\widetilde{\Theta}(r^2)$ copies suffice [UNWT'25]

[UNWT'25] – Utsumi, Nakata, Wang, Takagi. Quantum algorithms for the Uhlmann transformation. (2025)

Limitations of random purification

Problem (Fidelity estimation)
Given: n copies of $\rho \in \mathbb{C}^{d\times d}$ and n copies of $\sigma \in \mathbb{C}^{d\times d}$
Output: estimate of $F(\rho,\sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$

If ρ and σ both have rank at most r, then $\widetilde{\Theta}(r^2)$ copies suffice [UNWT'25]

Q: Can we see this again with the random purification channel?

[UNWT'25] – Utsumi, Nakata, Wang, Takagi. Quantum algorithms for the Uhlmann transformation. (2025)

Limitations of random purification

Attempt 1:

$$(\rho \otimes \sigma)^{\otimes n} \xrightarrow{\mathcal{P}^{(r^2)}} \left|\phi^{\rho\otimes\sigma}\rangle\langle\phi^{\rho\otimes\sigma}\right|^{\otimes n} \xrightarrow{\mathrm{tr}_1} \tau_0^{\otimes n} \qquad \tau_0 \in \mathbb{C}^{r^2\times r^2}, \quad \mathrm{spec}(\rho \otimes \sigma) = \mathrm{spec}(\tau_0)$$

Limitations of random purification

Attempt 1:

$$(\rho \otimes \sigma)^{\otimes n} \xrightarrow{\mathcal{P}^{(r^2)}} \left|\phi^{\rho\otimes\sigma}\rangle\langle\phi^{\rho\otimes\sigma}\right|^{\otimes n} \xrightarrow{\mathrm{tr}_1} \tau_0^{\otimes n} \qquad \tau_0 \in \mathbb{C}^{r^2\times r^2}, \quad \mathrm{spec}(\rho\otimes\sigma) = \mathrm{spec}(\tau_0)$$

Attempt 2:

$$\rho^{\otimes n} \xrightarrow{\mathcal{P}^{(r)}} |\phi^{\rho}\rangle\langle\phi^{\rho}|^{\otimes n} \xrightarrow{\mathrm{tr}_1} \rho_0^{\otimes n} \qquad \rho_0 \in \mathbb{C}^{r\times r}, \quad \mathrm{spec}(\rho) = \mathrm{spec}(\rho_0)$$

$$\sigma^{\otimes n} \xrightarrow{\mathcal{P}^{(r)}} |\phi^{\sigma}\rangle\langle\phi^{\sigma}|^{\otimes n} \xrightarrow{\mathrm{tr}_1} \sigma_0^{\otimes n} \qquad \sigma_0 \in \mathbb{C}^{r\times r}, \quad \mathrm{spec}(\sigma) = \mathrm{spec}(\sigma_0)$$

Limitations of random purification

Attempt 1:

$$(\rho \otimes \sigma)^{\otimes n} \xrightarrow{\mathcal{P}^{(r^2)}} \big|\phi^{\rho\otimes\sigma}\rangle\langle\phi^{\rho\otimes\sigma}\big|^{\otimes n} \xrightarrow{\operatorname{tr}_1} \tau_0^{\otimes n} \qquad \tau_0 \in \mathbb{C}^{r^2\times r^2}, \quad \operatorname{spec}(\rho\otimes\sigma) = \operatorname{spec}(\tau_0)$$

Attempt 2:

$$\rho^{\otimes n} \xrightarrow{\mathcal{P}^{(r)}} |\phi^{\rho}\rangle\langle\phi^{\rho}|^{\otimes n} \xrightarrow{\operatorname{tr}_1} \rho_0^{\otimes n} \qquad \rho_0 \in \mathbb{C}^{r\times r}, \quad \operatorname{spec}(\rho) = \operatorname{spec}(\rho_0)$$

$$\sigma^{\otimes n} \xrightarrow{\mathcal{P}^{(r)}} |\phi^{\sigma}\rangle\langle\phi^{\sigma}|^{\otimes n} \xrightarrow{\operatorname{tr}_1} \sigma_0^{\otimes n} \qquad \sigma_0 \in \mathbb{C}^{r\times r}, \quad \operatorname{spec}(\sigma) = \operatorname{spec}(\sigma_0)$$

Problem: both approaches throw away information about the eigenbases of ρ and σ

Dimension reduction: key idea

Pick a different channel $\mathcal{R}$ with the action

$$\begin{tikzcd}
\rho^{\otimes n} \arrow[r, "\mathcal{P}^{(r)}"] \arrow[rr, bend right, "\mathcal{R}"'] & |\phi^\rho\rangle\langle\phi^\rho|^{\otimes n} \arrow[r, "\mathrm{tr}_1"] & \rho_0^{\otimes n}
\end{tikzcd} \qquad \rho_0 \in \mathbb{C}^{r\times r}, \quad \mathrm{spec}(\rho) = \mathrm{spec}(\rho_0)$$

Dimension reduction: key idea

Pick a different channel $\mathcal{R}$ with the action

$$\begin{tikzcd} \rho^{\otimes n} \arrow[r, "\mathcal{P}^{(r)}"] \arrow[rr, bend right, "\mathcal{R}"'] & |\phi^\rho\rangle\langle\phi^\rho|^{\otimes n} \arrow[r, "\mathrm{tr}_1"] & \rho_0^{\otimes n} \end{tikzcd} \qquad \rho_0 \in \mathbb{C}^{r\times r}, \quad \mathrm{spec}(\rho) = \mathrm{spec}(\rho_0)$$

Then hopefully we also have

$$(\rho \otimes \sigma)^{\otimes n} \xrightarrow{\mathcal{R}} (\rho_0 \otimes \sigma_0)^{\otimes n}$$

where ρ_0, σ_0 have rank $O(r)$, *and* contain information about the eigenbases of ρ, σ

Dimension reduction channel

Let $k \leq d$

Dimension reduction channel

Let $k \leq d$

Let $W_0\colon \mathbb{C}^k \to \mathbb{C}^d$ be the isometry $W_0\colon |i\rangle \mapsto |i\rangle$ for all $i = 1, \ldots, k$

Dimension reduction channel

Let $k \leq d$

Let $W_0 : \mathbb{C}^k \to \mathbb{C}^d$ be the isometry $W_0 : |i\rangle \mapsto |i\rangle$ for all $i = 1, \dots, k$

Let $\boldsymbol{W} \equiv \boldsymbol{U} W_0$ where $\boldsymbol{U} \in \mathbb{C}^{d \times d}$ is Haar-random

Dimension reduction channel

Let $k \leq d$

Let $W_0 : \mathbb{C}^k \to \mathbb{C}^d$ be the isometry $W_0 : |i\rangle \mapsto |i\rangle$ for all $i = 1, \dots, k$

Let $\boldsymbol{W} \equiv \boldsymbol{U} W_0$ where $\boldsymbol{U} \in \mathbb{C}^{d \times d}$ is Haar-random

Let $M^{(n)} = \mathbb{E}\left(\boldsymbol{W}\boldsymbol{W}^\dagger\right)^{\otimes n}$

Dimension reduction channel

Let $k \leq d$

Let $W_0 : \mathbb{C}^k \to \mathbb{C}^d$ be the isometry $W_0 : |i\rangle \mapsto |i\rangle$ for all $i = 1, \dots, k$

Let $\boldsymbol{W} \equiv \boldsymbol{U} W_0$ where $\boldsymbol{U} \in \mathbb{C}^{d \times d}$ is Haar-random

Let $M^{(n)} = \mathbb{E}\left(\boldsymbol{W}\boldsymbol{W}^\dagger\right)^{\otimes n}$

Definition (Dimension reduction map)

$$\mathcal{R} : \mathrm{L}\left(\left(\mathbb{C}^d\right)^{\otimes n}\right) \to \mathrm{L}\left(\left(\mathbb{C}^k\right)^{\otimes n}\right)$$

$$\mathcal{R}(X) = \mathbb{E}\left[\left(\boldsymbol{W}^\dagger\right)^{\otimes n} M^{-1/2} X M^{-1/2} \boldsymbol{W}^{\otimes n}\right]$$

(when $k = d$, this is just a Haar twirl)

Dimension reduction channel

Let $k \leq d$

Let $W_0 : \mathbb{C}^k \to \mathbb{C}^d$ be the isometry $W_0 : |i\rangle \mapsto |i\rangle$ for all $i = 1, \ldots, k$

Let $\boldsymbol{W} \equiv \boldsymbol{U} W_0$ where $\boldsymbol{U} \in \mathbb{C}^{d \times d}$ is Haar-random

Let $M^{(n)} = \mathbb{E}\left(\boldsymbol{W}\boldsymbol{W}^\dagger\right)^{\otimes n}$

Definition (Dimension reduction map)

$$\mathcal{R} : \mathrm{L}\left(\left(\mathbb{C}^d\right)^{\otimes n}\right) \to \mathrm{L}\left(\left(\mathbb{C}^k\right)^{\otimes n}\right)$$

$$\mathcal{R}(X) = \mathbb{E}\left[\left(\boldsymbol{W}^\dagger\right)^{\otimes n} M^{-1/2} X M^{-1/2} \boldsymbol{W}^{\otimes n}\right]$$

(when $k = d$, this is just a Haar twirl)

Theorem

For any isometry $W : \mathbb{C}^k \to \mathbb{C}^d$ it holds that

$$\mathcal{R}\left(W^{\otimes n} X_0 \left(W^\dagger\right)^{\otimes n}\right) = \mathbb{E}_{\boldsymbol{U} \sim \mathbb{U}(k)} \boldsymbol{U}^{\otimes n} X_0 \left(\boldsymbol{U}^\dagger\right)^{\otimes n}$$

Examples

Theorem

For any isometry $W : \mathbb{C}^k \to \mathbb{C}^d$ it holds that

$$\mathcal{R}\left(W^{\otimes n} X_0 (W^\dagger)^{\otimes n}\right) = \mathop{\mathbb{E}}_{\boldsymbol{U}\sim\mathbb{U}(k)} \boldsymbol{U}^{\otimes n} X_0 (\boldsymbol{U}^\dagger)^{\otimes n}$$

1) $X = \rho^{\otimes n}$ for some rank-r ρ. Set $k = r$.

$$\mathcal{R}(\rho^{\otimes n}) = \mathop{\mathbb{E}}_{\boldsymbol{U}\sim\mathbb{U}(r)} (\boldsymbol{U}\rho_0\boldsymbol{U}^\dagger)^{\otimes n}, \qquad \mathrm{spec}(\rho_0) = \mathrm{spec}(\rho)$$

Examples

Theorem

For any isometry $W : \mathbb{C}^k \to \mathbb{C}^d$ it holds that

$$\mathcal{R}\left(W^{\otimes n} X_0 (W^\dagger)^{\otimes n}\right) = \mathop{\mathbb{E}}_{\boldsymbol{U}\sim\mathbb{U}(k)} \boldsymbol{U}^{\otimes n} X_0 (\boldsymbol{U}^\dagger)^{\otimes n}$$

1) $X = \rho^{\otimes n}$ for some rank-r ρ. Set $k = r$.

$$\mathcal{R}(\rho^{\otimes n}) = \mathop{\mathbb{E}}_{\boldsymbol{U}\sim\mathbb{U}(r)} (\boldsymbol{U}\rho_0\boldsymbol{U}^\dagger)^{\otimes n}, \qquad \mathrm{spec}(\rho_0) = \mathrm{spec}(\rho)$$

2) $X = \rho^{\otimes n} \otimes \sigma^{\otimes n}$ for some ρ, σ with ranks r_1, r_2 respectively. Set $k = r_1 + r_2$, $n \to 2n$

$$\mathcal{R}(\rho^{\otimes n} \otimes \sigma^{\otimes n}) = \mathop{\mathbb{E}}_{\boldsymbol{U}\sim\mathbb{U}(k)} \left[(\boldsymbol{U}\rho_0\boldsymbol{U}^\dagger)^{\otimes n} \otimes (\boldsymbol{U}\sigma_0\boldsymbol{U}^\dagger)^{\otimes n}\right]$$

where $\rho = W\rho_0 W^\dagger$ and $\sigma = W\sigma_0 W^\dagger$ for an isometry $W : \mathbb{C}^k \to \mathbb{C}^d$

Application to learning symmetric properties

A straightforward “baseline” strategy: **random dimension reduction + tomography**

Application to learning symmetric properties

A straightforward “baseline” strategy: **random dimension reduction + tomography**

For ρ, σ with ranks at most r,

$$\rho^{\otimes n} \otimes \sigma^{\otimes n} \xrightarrow{\mathcal{R}} \rho_0^{\otimes n} \otimes \sigma_0^{\otimes n} \xrightarrow{\text{tomography}} \hat{\rho}_0, \hat{\sigma}_0 \longrightarrow \text{estimate properties}$$

$$\mathcal{R}(\rho^{\otimes n} \otimes \sigma^{\otimes n}) = \mathop{\mathbb{E}}_{\boldsymbol{U} \sim \mathbb{U}(k)} \left[(\boldsymbol{U} \rho_0 \boldsymbol{U}^\dagger)^{\otimes n} \otimes (\boldsymbol{U} \sigma_0 \boldsymbol{U}^\dagger)^{\otimes n} \right]$$

If $f(\rho, \sigma)$ is symmetric and continuous, so that $f(\hat{\rho}_0, \hat{\sigma}_0) \approx f(\rho, \sigma)$, then $n = O(r^2)$ copies suffice.

Application to learning symmetric properties

Estimation task	Best prior	**This work**
Trace distance	$O(r^2 \cdot \log^2(1/\varepsilon)/\varepsilon^4)$ [WZ24a; CWZ25]	$O(r^2/\varepsilon^2)$
Fidelity	$O(r^2 \cdot \log^2(1/\varepsilon)/\varepsilon^4)^*$ [UNWT25]	$O(r^2/\varepsilon^2)$
α-Tsallis relative entropy, $0 < \alpha < 1/2$	$O(r^{2+2\alpha}/\varepsilon^{2/\alpha+2/(1-\alpha)})$ [CWZ25]	$O(r^2/\varepsilon^{1/\alpha})$
Squared Hellinger distance	$O(r^3 \cdot \log^2(r/\varepsilon)/\varepsilon^8)$ [CWZ25]	$O(r^2/\varepsilon^2)$

Proof sketch

Definition (Dimension reduction map)

$$\mathcal{R}\colon \mathrm{L}\left(\left(\mathbb{C}^d\right)^{\otimes n}\right) \to \mathrm{L}\left(\left(\mathbb{C}^k\right)^{\otimes n}\right)$$

$$\mathcal{R}(X) = \mathbb{E}\left[\left(\boldsymbol{W}^\dagger\right)^{\otimes n} M^{-1/2} X M^{-1/2} \boldsymbol{W}^{\otimes n}\right]$$

Theorem

For any isometry $W\colon \mathbb{C}^k \to \mathbb{C}^d$ it holds that

$$\mathcal{R}\left(W^{\otimes n} X_0 \left(W^\dagger\right)^{\otimes n}\right) = \mathop{\mathbb{E}}_{\boldsymbol{U}\sim\mathbb{U}(k)} \boldsymbol{U}^{\otimes n} X_0 \left(\boldsymbol{U}^\dagger\right)^{\otimes n}$$

$$\mathcal{R}(X) = \mathbb{E}\left[\left(\boldsymbol{W}^\dagger\right)^{\otimes n} M^{-1/2} X M^{-1/2} \boldsymbol{W}^{\otimes n}\right]$$

Proof sketch

Definition (Dimension reduction map)

$$\mathcal{R}\colon \mathrm{L}\left(\left(\mathbb{C}^d\right)^{\otimes n}\right) \to \mathrm{L}\left(\left(\mathbb{C}^k\right)^{\otimes n}\right)$$

$$\mathcal{R}(X) = \mathbb{E}\left[\left(\boldsymbol{W}^\dagger\right)^{\otimes n} M^{-1/2} X M^{-1/2} \boldsymbol{W}^{\otimes n}\right]$$

Theorem

For any isometry $W\colon \mathbb{C}^k \to \mathbb{C}^d$ it holds that

$$\mathcal{R}\left(W^{\otimes n} X_0 \left(W^\dagger\right)^{\otimes n}\right) = \mathop{\mathbb{E}}_{\boldsymbol{U}\sim\mathbb{U}(k)} \boldsymbol{U}^{\otimes n} X_0 \left(\boldsymbol{U}^\dagger\right)^{\otimes n}$$

$$\begin{aligned}\mathcal{R}(X) &= \mathbb{E}\left[\left(\boldsymbol{W}^\dagger\right)^{\otimes n} M^{-1/2} X M^{-1/2} \boldsymbol{W}^{\otimes n}\right] \\ &= \mathop{\mathbb{E}}_{\boldsymbol{V}\sim\mathbb{U}(k)} \boldsymbol{V}^{\otimes n}\left[\left(\boldsymbol{W}^\dagger\right)^{\otimes n} M^{-1/2} X M^{-1/2} \boldsymbol{W}^{\otimes n}\right]\left(\boldsymbol{V}^\dagger\right)^{\otimes n}\end{aligned}$$

Proof sketch

Definition (Dimension reduction map)

$$\mathcal{R}\colon \mathrm{L}\left(\left(\mathbb{C}^d\right)^{\otimes n}\right) \to \mathrm{L}\left(\left(\mathbb{C}^k\right)^{\otimes n}\right)$$

$$\mathcal{R}(X) = \mathbb{E}\left[\left(\boldsymbol{W}^\dagger\right)^{\otimes n} M^{-1/2} X M^{-1/2} \boldsymbol{W}^{\otimes n}\right]$$

Theorem

For any isometry $W\colon \mathbb{C}^k \to \mathbb{C}^d$ it holds that

$$\mathcal{R}\left(W^{\otimes n} X_0 \left(W^\dagger\right)^{\otimes n}\right) = \mathop{\mathbb{E}}_{\boldsymbol{U}\sim\mathbb{U}(k)} \boldsymbol{U}^{\otimes n} X_0 \left(\boldsymbol{U}^\dagger\right)^{\otimes n}$$

$$\begin{aligned}
\mathcal{R}(X) &= \mathbb{E}\left[\left(\boldsymbol{W}^\dagger\right)^{\otimes n} M^{-1/2} X M^{-1/2} \boldsymbol{W}^{\otimes n}\right] \\
&= \mathop{\mathbb{E}}_{\boldsymbol{V}\sim\mathbb{U}(k)} \boldsymbol{V}^{\otimes n} \left[\left(\boldsymbol{W}^\dagger\right)^{\otimes n} M^{-1/2} X M^{-1/2} \boldsymbol{W}^{\otimes n}\right] \left(\boldsymbol{V}^\dagger\right)^{\otimes n} \\
&= \sum_{\pi,\sigma\in S_n} \mathrm{Wg}\,(k,\sigma^{-1}\pi) \mathbb{E}\,\mathrm{tr}\left(F^k_{\sigma^{-1}} \left(\boldsymbol{W}^\dagger\right)^{\otimes n} M^{-1/2} X M^{-1/2} \boldsymbol{W}^{\otimes n}\right) F^k_\pi
\end{aligned}$$

Proof sketch

Definition (Dimension reduction map)

$$\mathcal{R}\colon \mathrm{L}\left(\left(\mathbb{C}^d\right)^{\otimes n}\right) \to \mathrm{L}\left(\left(\mathbb{C}^k\right)^{\otimes n}\right)$$

$$\mathcal{R}(X) = \mathbb{E}\left[\left(\boldsymbol{W}^\dagger\right)^{\otimes n} M^{-1/2} X M^{-1/2} \boldsymbol{W}^{\otimes n}\right]$$

Theorem

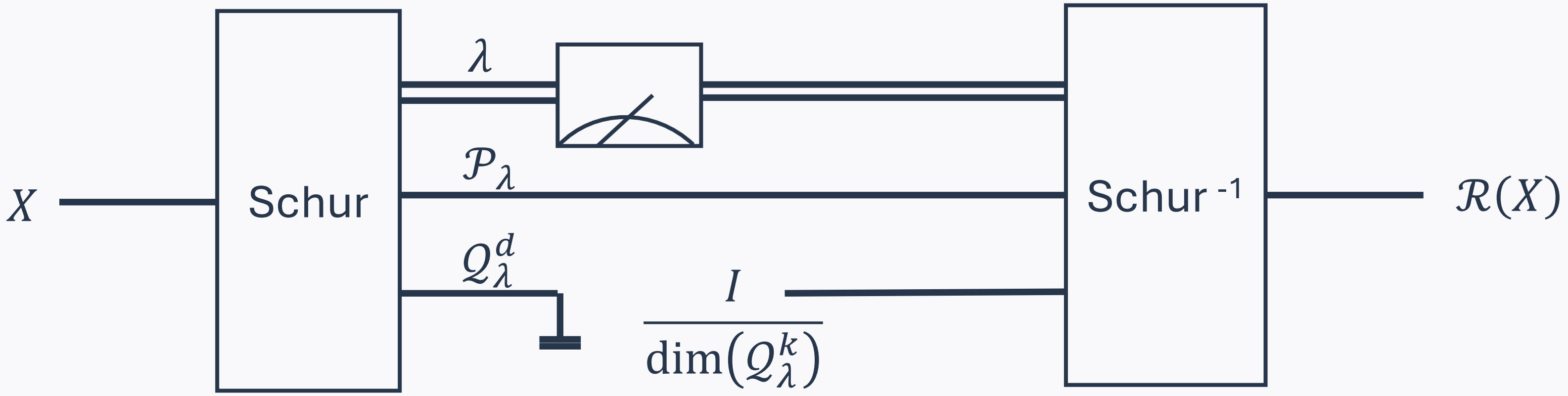
For any isometry $W\colon \mathbb{C}^k \to \mathbb{C}^d$ it holds that

$$\mathcal{R}\left(W^{\otimes n} X_0 \left(W^\dagger\right)^{\otimes n}\right) = \mathbb{E}_{\boldsymbol{U}\sim\mathbb{U}(k)} \boldsymbol{U}^{\otimes n} X_0 \left(\boldsymbol{U}^\dagger\right)^{\otimes n}$$

$$\begin{aligned}
\mathcal{R}(X) &= \mathbb{E}\left[\left(\boldsymbol{W}^\dagger\right)^{\otimes n} M^{-1/2} X M^{-1/2} \boldsymbol{W}^{\otimes n}\right] \\
&= \mathbb{E}_{\boldsymbol{V}\sim\mathbb{U}(k)} \boldsymbol{V}^{\otimes n}\left[\left(\boldsymbol{W}^\dagger\right)^{\otimes n} M^{-1/2} X M^{-1/2} \boldsymbol{W}^{\otimes n}\right]\left(\boldsymbol{V}^\dagger\right)^{\otimes n} \\
&= \sum_{\pi,\sigma\in S_n} \mathrm{Wg}\,(k,\sigma^{-1}\pi)\mathbb{E}\,\mathrm{tr}\left(F^k_{\sigma^{-1}}\left(\boldsymbol{W}^\dagger\right)^{\otimes n} M^{-1/2} X M^{-1/2} \boldsymbol{W}^{\otimes n}\right) F^k_\pi \\
&= \sum_{\pi,\sigma\in S_n} \mathrm{Wg}\,(k,\sigma^{-1}\pi)\,\mathrm{tr}\left(F^d_{\sigma^{-1}} X\right) F^k_\pi
\end{aligned}$$

Efficient implementation

$$\left(\mathbb{C}^d\right)^{\otimes n} \cong \bigoplus_{\lambda \vdash n} \mathcal{P}_\lambda \otimes \mathcal{Q}_\lambda^d$$



See also [YSM'23]

[YSM'23] – Yoshida, Soeda, Murao. Universal construction of decoders from encoding black boxes. (Quantum 7, 2023)

Random purifications revisited

Recall the *Choi-Jamiolkowski isomorphism*

$$J_{\mathcal{N}} = (\mathrm{id} \otimes \mathcal{N})(|\Gamma\rangle\langle\Gamma|), \quad |\Gamma\rangle = \sum_{i=1}^{d} |i\rangle |\, i\rangle$$

Random purifications revisited

Recall the *Choi-Jamiolkowski isomorphism*

$$J_{\mathcal{N}} = (\mathrm{id} \otimes \mathcal{N})(|\Gamma\rangle\langle\Gamma|), \qquad |\Gamma\rangle = \sum_{i=1}^{d} |i\rangle|\, i\rangle$$

Action of $\mathcal{N}$ is recovered through $\mathcal{N}(X) = \mathrm{tr}_1\big(\underbrace{J_{\mathcal{N}}(X^T \otimes I)}_{\text{Usually, not CP}}\big).$

Random purifications revisited

Recall the *Choi-Jamiolkowski isomorphism*

$$J_{\mathcal{N}} = (\mathrm{id} \otimes \mathcal{N})(|\Gamma\rangle\langle\Gamma|), \quad |\Gamma\rangle = \sum_{i=1}^{d} |i\rangle|\, i\rangle$$

Action of $\mathcal{N}$ is recovered through $\mathcal{N}(X) = \mathrm{tr}_1\big(J_{\mathcal{N}} \underbrace{(X^T \otimes I)}_{\text{Usually, not CP}}\big)$.

This means $\mathcal{R}(X) = \mathrm{tr}_1\big(J_{\mathcal{R}}(X^T \otimes I)\big)$.

Random purifications revisited

Recall the *Choi-Jamiolkowski isomorphism*

$$J_{\mathcal{N}} = (\mathrm{id} \otimes \mathcal{N})(|\Gamma\rangle\langle\Gamma|), \quad |\Gamma\rangle = \sum_{i=1}^{d} |i\rangle|\, i\rangle$$

Action of $\mathcal{N}$ is recovered through $\mathcal{N}(X) = \mathrm{tr}_1\big(\underbrace{J_{\mathcal{N}}(X^T \otimes I)}_{\text{Usually, not CP}}\big)$.

This means $\mathcal{R}(X) = \mathrm{tr}_1\big(J_{\mathcal{R}}(X^T \otimes I)\big)$.

Q: what is $\mathcal{P}(X) \equiv J_{\mathcal{R}}(X^T \otimes I)$?

Random purifications revisited

Recall the *Choi-Jamiolkowski isomorphism*

$$J_{\mathcal{N}} = (\mathrm{id} \otimes \mathcal{N})(|\Gamma\rangle\langle\Gamma|), \quad |\Gamma\rangle = \sum_{i=1}^{d} |i\rangle|\, i\rangle$$

Action of $\mathcal{N}$ is recovered through $\mathcal{N}(X) = \mathrm{tr}_1\big(\underbrace{J_{\mathcal{N}}(X^T \otimes I)}_{\text{Usually, not CP}}\big)$.

This means $\mathcal{R}(X) = \mathrm{tr}_1\big(J_{\mathcal{R}}(X^T \otimes I)\big)$.

Q: what is $\mathcal{P}(X) \equiv J_{\mathcal{R}}(X^T \otimes I)$?

A: the random purification channel, when restricted to *exchangeable* inputs X, e.g., $\rho^{\otimes n}$

Quantum tomography revisited

Optimal quantum tomography with $n = \Theta(dr)$ copies no longer requires representation theory to describe.

$$\rho^{\otimes n} \xrightarrow{\mathcal{P}^{(r)}} |\phi^\rho\rangle\langle\phi^\rho|^{\otimes n} \xrightarrow{\text{Pure tomography}} |\hat{\phi}^\rho\rangle$$

(Observed in [PSTW'26])

Quantum tomography revisited

Optimal quantum tomography with $n = \Theta(dr)$ copies no longer requires representation theory to describe.

$$\rho^{\otimes n} \xrightarrow{\mathcal{P}^{(r)}} |\phi^\rho\rangle\langle\phi^\rho|^{\otimes n} \xrightarrow{\text{Pure tomography}} |\hat{\phi}^\rho\rangle$$

(Observed in [PSTW'26])

$|\phi^\rho\rangle$ is D-dimensional with $D = dr$.

Pure tomography with $n = O(D)$ copies: just uses church of the symmetric subspace [Har13].

$$\begin{aligned}\int \mathrm{tr}\left(D[n]|u\rangle\langle u|^{\otimes n} \cdot |\psi\rangle\langle\psi|^{\otimes n}\right)|\langle u|\psi\rangle|^2 du &= D[n]\mathrm{tr}\left(\int |u\rangle\langle u|^{\otimes n+1}\, du \cdot |\psi\rangle\langle\psi|^{\otimes n+1}\right) \\ &= \frac{D[n]}{D[n+1]} \\ &\approx 1 - \frac{D}{n}\end{aligned}$$

[PSTW'26] – Pelecanos, Spilecki, Tang, Wright. Mixed state tomography reduces to pure state tomography. (2025)

[Har13] – Aram Harrow. The Church of the symmetric subspace. (2013)

Conclusion

- Random dimension reduction sets baseline for the sample complexity of learning symmetric quantum properties. When can we beat it?
  - First example recently shown in [PSTW'26].
- Our construction also shows that it can be useful to apply the Schur transform to states of the form $\rho^{\otimes a} \otimes \sigma^{\otimes b}$
- Minimum vs maximum rank: for fidelity estimation, natural dependence is on the minimum rank. Can we derive an upper bound of $O\left(r_{\min}^2/\varepsilon^2\right)$?
- Robustness: approximate, not exact, low rank is a more physically realistic assumption.

[PSTW'26] – Pelecanos, Spilecki, Tang, Wright. The Keyl-Werner algorithm is not optimal for spectrum estimation (2026)